Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
08 JUL 2013	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Multinational Experiment 7: Cyber Situation Awareness Technologies Used in Locked Shield 2012	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

As in the real world, the lack of timely reports on network incidents has been a major obstacle in establishing situation awareness in cyber security exercises. The security teams are too busy handling the incidents to create detailed reports. However, the observations and actions made by local experts are crucial to well-informed high-level decisions. At the Locked Shield 2012 exercise, Clarified networks was responsible for providing SA solutions and building the Finnish situation room. AbuseSA, a collaborative system, which combines instant messaging, wikis and real-time visualizations to provide actionable situation awareness, was implemented. To encourage security teams to report incidents, a CDX extension to AbuseSA, which allows users to quickly report incident using instant messaging, was introduced. The overall execution consisted of providing the technical solution and helping the exercise organizers to implement the supporting workflows. The results of the exercise were positive with all teams using the functionality to report incidents.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**9**	

Situation Awareness Technologies Used in Locked Shield 2012

Contents

1. Executive Summary

As in the real world, the lack of timely reports on network incidents has been a major obstacle in establishing situation awareness in cyber security exercises. The security teams are too busy handling the incidents to create detailed reports. However, the observations and actions made by local experts are crucial to well-informed high-level decisions.

At the Locked Shield 2012 exercise, Clarified networks was responsible for providing SA solutions and building the Finnish situation room. AbuseSA, a collaborative system, which combines instant messaging, wikis and real-time visualizations to provide actionable situation awareness, was implemented. To encourage security teams to report incidents, a CDX extension to AbuseSA, which allows users to quickly report incident using instant messaging, was introduced. The overall execution consisted of providing the technical solution and helping the exercise organizers to implement the supporting workflows. The results of the exercise were positive with all teams using the functionality to report incidents.

1.1. About the Solution

AbuseSA is a collaborative solution, which combines different tools and workflows seamlessly. AbuseSA is a product designed for collecting, aggregating, normalizing information from various sources, to provide actionable reports and situation awareness visualizations. The CDX extension is a module, which enables domain experts to contribute insight into the situation awareness.

At Locked Shields 2012, AbuseSA was used to establish situational awareness. Instant Messaging, Wikis and different visualization tools have traditionally provided point-solutions to specific challenges, but AbuseSA with CDX extensions enabled the flow of information from the low-level reports to high-level visualizations. The *Instant Messaging based microblog-style reports* removed reporting barriers. The *Semantic Wiki-based* collaboration environment captured the reports, displayed incidents in tabular views and provided supporting functions, such as instructions. *Real-time situation visualizations* provided an overview of the game activity and *Network situation awareness tools* were used to visualize network activity during the game and to document critical assets. This information was then used to augment incident reports with contextual information.

The AbuseSA technology can be used by Cyber Centers and SOCs to perform their roles as specified in the Cyber Situational Awareness Standard Operating Procedure. In Locked Shield the solution was deployed to serve CDX organization, where the organization model was slightly different.

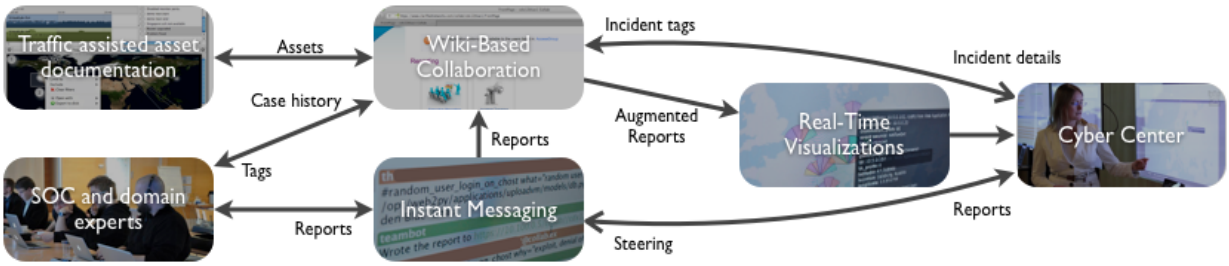


Figure 1: *AbuseSA with CDX extensions was used to establish situation awareness at Locked Shields 2012. The product integrates several technologies.*

1.2. About the Vendor

The solution was provided by Clarified Networks Oy, a Codenomicon Group company.

Codenomicon Oy is known for its innovative products and services used to secure network equipment, software, complex systems and critical infrastructure against unknown vulnerabilities and rapidly changing threats. Clarified Networks is a pioneer in collaborative network analysis, Internet abuse reporting and visualization, and critical infrastructure monitoring.

1.3. About the Exercise

The Locked Shields 2012 exercise consisted of nine Blue Teams whose task was to defend their respective networks and report their findings to the CERT Team on the Cyber Center. The Red Team was setup to attack the Blue Teams and provide real incidents for the exercise. Blue Teams were encouraged to share information with each other and required to inform the Cyber Center by microblogging and mandatory regular manual reporting. A per team Intrusion Detection System was also setup to feed automated alerts to the Cyber Center.

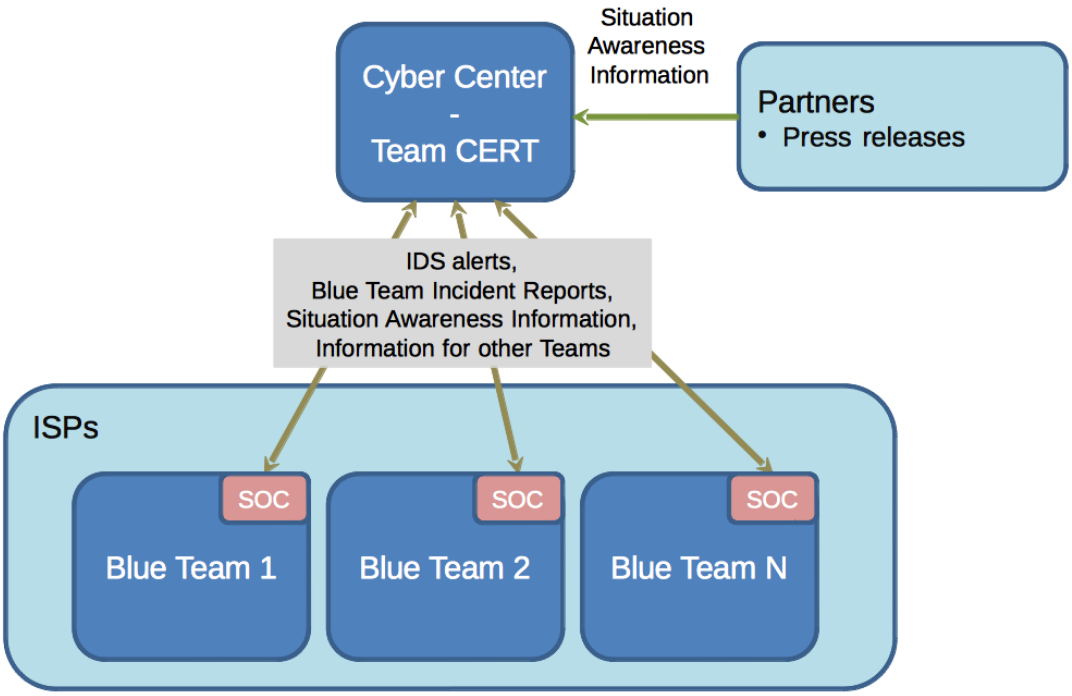


Figure 2: *How the SOP was implemented in CDX.*

2. Challenges the Solution was Set Out to Resolve

The role the Yellow Team was to experiment with different technologies to create situational awareness or a common operating picture that could be used in a national Cyber Center. Such an operating picture should consist not only of network level incident information but also a higher level operational view of what is going on. The objective of the Yellow Team was to be able help Blue Teams in coordinating efforts to repel the attacks and to have a clear overall situational awareness at all times. Different kinds of visualisation methods were used to achieve the objective.

Previous exercises have demonstrated how difficult it is to gain situation awareness in a time of crisis. Firstly, traditional technical sources are not enough to produce adequate situation awareness. Secondly, local experts, who have the needed expertise, are too busy mitigating the issues to produce detailed, good quality reports. Finally, dedicated resources for reporting are rarely available.

A reverse approach was chosen to build situation awareness. A typical obstacle in technical exercises is the lack of timely reports providing information on observations, decisions and actions made by local domain experts. This kind of information is crucial to making well-informed high-level decisions. In the exercise, the first priority was to remove all barriers preventing the flow of good quality information from the lowest, most technical and detailed level to the highest, most abstract level. This was achieved by enabling microblog style reporting using an instant messaging client. The second priority was to enhance the quality of the reports. This was done by using existing network asset documentation to augment the events. The information was then visualized to further assist the Cyber Center.

Below, the risks of failing to produce proper situation awareness are itemized. The mitigation mechanisms used at Locked Shield 2012 are also listed.

Risk	**Mitigation**
Technical data sources are not sufficient - or even applicable - for providing Cyber Center with situation awareness	Collect more contextual information from local experts
The poor signal/noise ratio of technical data sources combined with the complexity of modern systems renders it difficult to produce high-level information	Collect more contextual information from local experts
Video/Audio records labourious to follow and analyze	Capture information in textual form
Domain experts are too busy mitigating the damages to produce reports during a time of crisis	Remove the reporting overhead
Phenomenas are complex and the available information is often too incomplete to produce highly structured reports	Enforce minimal amount of structure
Unstructured data not suitable for providing situation awareness	Allow the Cyber Centers to tag information to produce more meaningful visualisations and to provide feedback to reporters
Workflows, terminology, requirements for Cyber Situation Awareness are unclear	Use a platform, which allows rapid prototyping of different worklows and allows changes in reporting mechanisms and visualizations.

Table 1: Risks and solutions to mitigate the risks.

3. Approach

3.1. Data Sources

Two kinds of data sources were used in the exercise; manual reporting and automated incidents alerts. Teams were required to write daily reports on the perceived incidents and activities done to counter them. Additionally, Cyber Center was provided with an automated feed of IDS alerts, originating from sensors monitoring Blue Team traffic.

3.1.1. Instant Messaging for Low-Overhead Reporting

The decision to use Instant Messaging for reporting was based on two earlier observations:

Firstly, a number of teams ranging from national CERTs to local computer incident response teams already use instant messaging for communication. Instant messaging makes it possible to quickly form virtual teams and share notes (e.g. IP-addresses, domain names, locations of malicious files etc.). Co-workers can easily copy and paste data from the instant messaging client for further analysis. In addition, the chat logs automatically produce notes and an investigation timeline.

Secondly, microblog services such as Twitter have taught people to quickly share small pieces of information. Similarly, the security teams' readiness to report could be improved by lowering the barrier to relate actions, decisions and observations. This assumption turned out to be correct. For the first time at a cyber security exercise, we observed reports flowing in from all the teams.

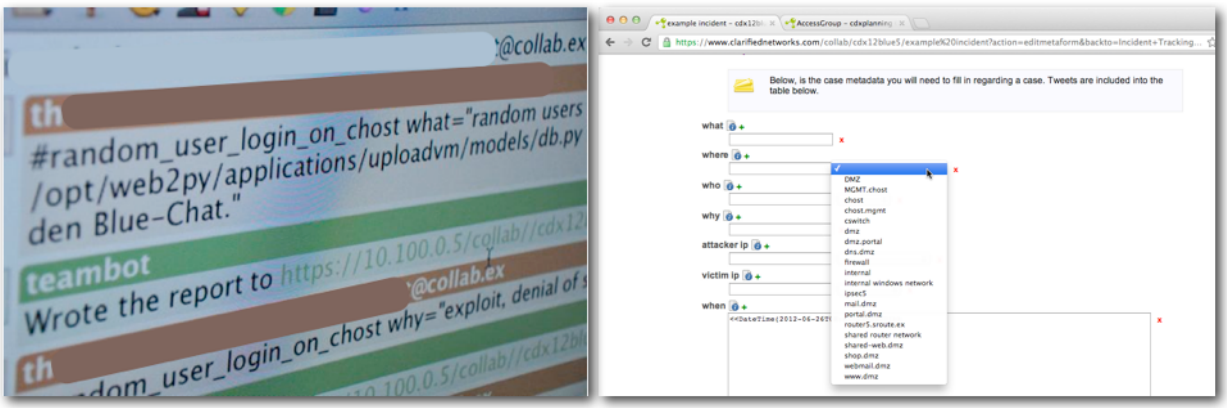


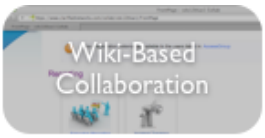
Figure 2: Teams used Instant Messaging for low-overhead and real-time reporting. A form-based alternative was also available.

3.1.2. Automated Techical level Sources

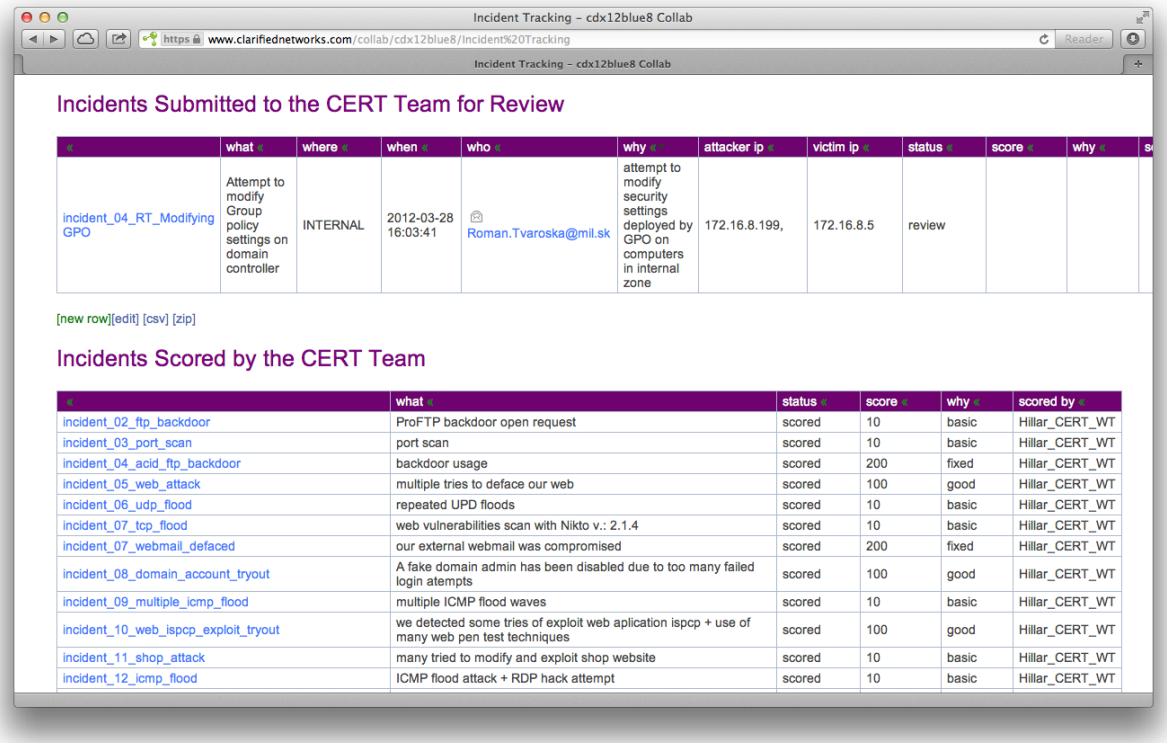
An IDS sensor was placed at each Blue Team to monitor traffic. The alerts raised by the sensors were sent to the Cyber Center to help develop the situational awareness. This was done to simulate a national or large organisation level monitoring solution that might be in place. The alerts were based on predefined attack signatures and consisted of detailed information about known attacks.

3.2. Result Representation / Visualization & Colaboration

3.2.1. Wiki-Based Collaboration Portal for Storing Semantic Data



While Instant Messaging is excellent for rapid information sharing and the timeline-based analysis of events, wikis provide other necessary functionalities. In the exercise, we used a Wiki-based collaboration environment to provide a table-format incident tracking system. The tracking system enabled the teams to see a list of their incidents. The white team had an overview of all incidents across the teams. The collaboration environment also allowed team members to share all types of attachments in a centralised manner.



	what	where	when	who	why	attacker ip	victim ip	status	score	why	
incident_04_RT_Modifying GPO	Attempt to modify Group policy settings on domain controller	INTERNAL	2012-03-28 16:03:41	Roman.Tvaroska@mil.sk	attempt to modify security settings deployed by GPO on computers in internal zone	172.16.8.199,	172.16.8.5	review			

	what	status	score	why	scored by
incident_02_ftp_backdoor	ProFTP backdoor open request	scored	10	basic	Hillar_CERT_WT
incident_03_port_scan	port scan	scored	10	basic	Hillar_CERT_WT
incident_04_acid_ftp_backdoor	backdoor usage	scored	200	fixed	Hillar_CERT_WT
incident_05_web_attack	multiple tries to deface our web	scored	100	good	Hillar_CERT_WT
incident_06_udp_flood	repeated UPD floods	scored	10	basic	Hillar_CERT_WT
incident_07_tcp_flood	web vulnerabilities scan with Nikto v.: 2.1.4	scored	10	basic	Hillar_CERT_WT
incident_07_webmail_defaced	our external webmail was compromised	scored	200	fixed	Hillar_CERT_WT
incident_08_domain_account_tryout	A fake domain admin has been disabled due to too many failed login atempts	scored	100	good	Hillar_CERT_WT
incident_09_multiple_icmp_flood	multiple ICMP flood waves	scored	10	basic	Hillar_CERT_WT
incident_10_web_ispcp_exploit_tryout	we detected some tries of exploit web aplication ispcp + use of many web pen test techniques	scored	100	good	Hillar_CERT_WT
incident_11_shop_attack	many tried to modify and exploit shop website	scored	10	basic	Hillar_CERT_WT
incident_12_icmp_flood	ICMP flood attack + RDP hack attempt	scored	10	basic	Hillar_CERT_WT

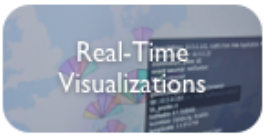
Figure 3: *Incident tracking functionality provided by the collaboration environment.*

The collaboration environment also contained document templates for executive reporting and reporting instructions. To enhance the quality of reporting the teams were encouraged to use the following keys. However, to avoid creating any barriers for reporting, using these keys was optional and using other keys was also allowed. The teams mostly used the keys *status*, *what*, *attacker ip* and *victim ip*.

what A free-form description of what has happened. **The most important thing to report!**
where Which network segment has been attacked, e.g. DMZ or INTERNAL
when When the event took place. This information is added automatically by the reporting system.
who Who handled the incident.
why What was the motivation of the attackers (if known).
attacker ip The IP the attackers used to perform the attack (can be several).
victim ip The IP of the attacked system (can be several).
status Once you are satisfied with your incident report, you can submit it to the CERT team for review by changing the status to **review**. Once the CERT Team has scored the incident, you will see it in the Figure 3. Please note that creating your own scores for incidents will lead to automatic disqualification.

Table 2: Optional keys in the reporting template.

3.2.2. Real-Time Visualizations for the Cyber Center



The AbuseSA enables the Cyber Center and the SOCs to share real-time visualizations of the situation awareness information. It is also possible that the Cyber Center has access to information across the various domains, while the SOCs only see data directly related to them.

The visualizations can be used to get a rapid overview of the situation and to spot abnormalities, such as missing or contradicting information. When abnormalities are spotted, the Cyber Center can use Instant Messaging to provide more information or to request further information from the SOCs, or even directly from the local experts. The figure below depicts a situation, where the Cyber Center observes that all the teams except one have registered scanning activity. In such a situation, the Cyber Center can instruct (direct) SOC to verify that their monitoring is working correctly, or to check, if they have seen any similar activity.

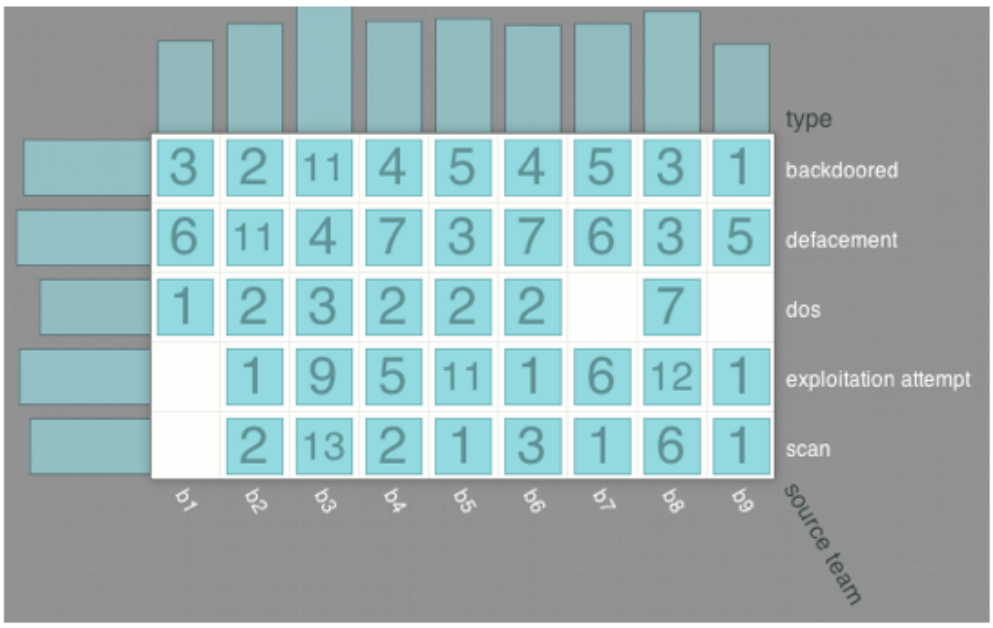
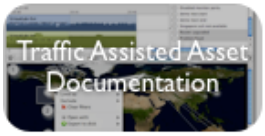


Figure 4: *Cyber Center spots an abnormality - all other teams except b1 have reported scanning activity.*

3.2.3. Network Situation Awareness for Traffic Assisted Asset Documentation



The main reason for deploying Network Situation Awareness tools in the exercise was to enable the automated augmentation of cyber asset incident reports. For example, if a report identifies the attack target with an IP-address, then other information such as network segments, names and the role of the asset can be augmented. Using this methodology also helps to keep the critical documentation up to date, as the information is routinely used.

Figure 5: *Analyzer provides traffic assisted and collaborative network asset documentation. The generated documentation was used for visualizing networks and augmenting incoming reports.*

AbuseSA solution comes with a tool for collaborative network analysis and documentation. Network owners can deploy sensors, which collect and index all the traffic in their networks. This data can then be viewed simultaneously with a tool called the Clarified Analyzer. The Analyzer provides visual and textual information about network events. It also allows the user to create documentation using real network traffic as a basis. The user can document network assets and freely choose the documented items, such as asset names, network zones, admins, roles and so forth. Network events can then be analyzed against the documentation. Undocumented assets and documentation that contradicts with the reality can quickly be pinpointed and fixed. The data is stored in the collaboration environment and it can also be used by other components of the AbuseSA. In addition, third party components can pull and push information relevant to the documented assets.

4. Conclusions

4.1. Benefits

The tools used in the exercise were helpful to enhance information exchange. Especially microblog-based reporting performed beyond expectations in terms of getting data from the teams. We expected that approximately half of the teams would start reporting once the barriers are removed. Instead, all the teams produced quick real-time reports. The quality of reports varied, but it was sufficient to form a basis for situation awareness. Teams were also able to collaborate with each other and share information regarding incidents and possible mitigations efforts. The technical solution was easy to use, sufficiently efficient and met the needs of the players.

The wiki-based collaboration tool was used successfully deliver mandatory summary reports at the end of the day. Collaboration was used for off-game activities as well, such as planning or incident tracking.

4.2. Shortcomings

Many different visualisation methods used during the exercise. Although visualisations were visually impressive, they failed to provide an overall situational awareness. They were helpful in clarifying certain individual incidents or providing a summary of statistics such as number of reports sent by the teams, but more emphasis should be placed on defining the use of different visualisations tools. None of the views were able to illustrate what was going on in general.

The Cyber Center wasn't able to actively give guidance to defending teams or coordinate the mitigating actions. The tools available would have made it possible, but they weren't fully utilised in that role.

4.3. Improvements

In order to create and maintain a comprehensive situational awareness, dedicated Cyber Center analysts seem to be needed for future exercises. They would be tasked with creating higher level reports for decision makers about the situation and steer the reporting of SOCs. To fully benefit from the visualisation tools, the Cyber Center should be able to define what kind of information and visualisations they would like to have to help them in maintaining a most useful common operating picture.

YTTechMNE7 (last edited 2012-12-04 10:10:47 by ?tomi.hasu@mil.fi)